

(3) Requesters should plainly display the words “Freedom of Information Act Request” on the lower left hand corner of the envelope to ensure prompt handling.

(b) [Reserved]

[56 FR 49685, Oct. 1, 1991, as amended at 57 FR 30904, July 13, 1992; 58 FR 63084, Nov. 30, 1993; 60 FR 18006, Apr. 10, 1995; 60 FR 35699, July 11, 1995; 61 FR 4885, Feb. 9, 1996; 61 FR 5510, Feb. 13, 1996; 64 FR 1131, Jan. 8, 1999]

#### APPENDIX C TO PART 290—FOR OFFICIAL USE ONLY

(a) General. Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public for one or more of the reasons cited in FOIA Exemptions 2 through 9 shall be considered as being for official use only. No other material shall be considered or marked “For Official Use Only” (FOUO). FOUO is not authorized as an anemic form of classification to protect national security interests.

(b) Prior FOUO Application. The prior application of FOUO markings is not a conclusive basis for withholding a record that is requested under the FOIA. When such a record is requested, the information in it shall be evaluated to determine whether, under current circumstances, FOIA exemptions apply in withholding the record or portions of it. If any exemption or exemptions apply or apply, it may nonetheless be released when it is determined that no governmental interest will be jeopardized by its release. (1) Historical Papers. Records such as notes, working papers, and drafts retained as historical evidence of Agency actions enjoy no special status apart from the exemptions under the FOIA.

(2) Time to Mark Records. The marking of records at the time of their creation provides notice of FOUO content and facilitates review when a record is requested under the FOIA. Records requested under the FOIA that do not bear such markings, shall not be assumed to be releasable without examination for the presence of information that requires continued protection and qualifies as exempt from public release.

(3) Distribution Statement. Information in a technical document that requires a distribution statement pursuant to DoD Directive 5230.24<sup>1</sup> shall bear that statement and may be marked FOUO, as appropriate.

(c) Markings. (1) Location of Markings. (i) An unclassified document containing FOUO information shall be marked “For Official Use Only” at the bottom on the outside of the front cover (if any), on each page con-

taining FOUO information, and on the outside of the back cover (if any).

(ii) Within a classified document, an individual page that contains both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page.

(iii) Within a classified document, an individual page that contains FOUO information but no classified information shall be marked “For Official Use Only” at the bottom of the page.

(iv) Other records, such as, photographs, films, tapes, or slides, shall be marked “For Official Use only” or “FOUO” in a manner that ensures that a recipient or viewer is aware of the status of the information therein.

(v) FOUO material transmitted outside the Department of Defense requires application of an expanded marking to explain the significance of the FOUO marking. This may be accomplished by typing or stamping the following statement on the record prior to transfer:

This document contains information  
EXEMPT FROM MANDATORY DISCLOSURE

Under the FOIA. Exemptions . . . . apply.

(2) Instructions for marking DCAA audit reports are contained in Chapter 10 of the Contract Audit Manual (CAM)<sup>2</sup>.

(3) DCAA Label 4, FOUO Cover Sheet. This form may be used to further identify FOUO information.

(d) Dissemination and Transmission. (1) Release and Transmission Procedures. Until FOUO status is terminated, the release and transmission instructions that follow apply:

(i) FOUO information may be disseminated within the Agency and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the Department of Defense. Recipients shall be made aware of the status of such information, and transmission shall be by means that preclude unauthorized public disclosure. Transmittal documents shall call attention to the presence of FOUO attachments.

(ii) Agency and DoD holders of FOUO information are authorized to convey such information to officials in other departments and agencies of the executive and judicial branches to fulfill a government function, except to the extent prohibited by the Privacy Act. Records thus transmitted shall be marked “For Official Use Only”, and the recipient shall be advised that the information has been exempted from public disclosure,

<sup>1</sup>Copies may be obtained, at cost, from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

<sup>2</sup>Copies may be obtained from the Defense Contract Audit Agency, Attn: CMO, 8725 John J. Kingman Road, Suite 2135, Fort Belvoir, VA 22060-6219.

pursuant to the FOIA, and that special handling instructions do or do not apply.

(iii) Release of FOUO information to Members of Congress is governed by DoD Directive 5400.4<sup>3</sup> Release to the GAO is governed by DoD Directive 7650.1<sup>4</sup> Records released to the Congress or GAO should be reviewed to determine whether the information warrants FOUO status. If not, prior FOUO markings shall be removed or effaced. If withholding criteria are met, the records shall be marked FOUO and the recipient provided an explanation for such exemption and marking. Alternatively, the recipient may be requested, without marking the record, to protect against its public disclosure for reasons that are explained.

(iv) Records or documents containing FOUO information will be transported between offices in such a manner as to preclude disclosure of the contents. First-class mail and ordinary parcel post may be used for transmission of FOUO information. The double envelope system required for classified material may be used when it is considered desirable to exclude examination by mail handling personnel. In such cases, the inner envelope should be addressed to the intended recipient by title or name and contain a statement that the envelope is to be opened by the addressee only.

(v) FOUO material prepared on personal computers or other data processing equipment should be password protected at origination.

(vi) Requests for Field Detachment sensitive information must be coordinated with the Director, Field Detachment, through Headquarters, DCAA.

(2) Transporting FOUO Information. Records containing FOUO information shall be transported in a manner that precludes disclosure of the contents. When not commingled with classified information, FOUO information may be sent via first-class mail or parcel post. Bulky shipments, such as distributions of FOUO Directives or testing materials, that otherwise qualify under postal regulations may be sent by fourth-class mail.

(3) Electrically Transmitted Messages. Each part of electrically transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text. Such messages shall be transmitted in accordance with communications security procedures in Allied Communication Publication 121 (U.S. Supp 1) for FOUO information.

(e) Safeguarding FOUO Information. (1) During Duty Hours. During normal working

hours, records determined to be FOUO shall be placed in an out-of-sight location if the work area is accessible to nongovernmental personnel.

(2) During Nonduty Hours. At the close of business, FOUO records shall be stored so as to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks, etc., is adequate when normal U.S. Government or Government-contractor internal building security is provided during nonduty hours. When such internal security control is not exercised, locked buildings or rooms normally provide adequate after hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked receptacles such as file cabinets, desks, or bookcases. FOUO records that are subject to the provisions of Public Law 86-36 shall meet the safeguards outlined for that group of records.

(3) Field audit offices located in contractor owned facilities will ensure that material marked FOUO is stored in a locked receptacle to which the contractor does not have access during nonduty hours.

(f) Termination, Disposal and Unauthorized Disclosures. (1) Termination. The originator or other competent authority, e.g., initial denial and appellate authorities, shall terminate "For Official Use Only" markings or status when circumstances indicate that the information no longer requires protection from public disclosure. When FOUO status is terminated, all known holders shall be notified, to the extent practical. Upon notification, holders shall efface or remove the "For Official Use Only" markings, but records in file or storage need not be retrieved solely for that purpose.

(2) Disposal. (i) Nonrecord copies of FOUO materials may be destroyed by tearing each copy into pieces to preclude reconstructing, and placing them in regular trash containers. When local circumstances or experience indicates that this destruction method is not sufficiently protective of FOUO information, local authorities may direct other methods but must give due consideration to the additional expense balanced against the degree of sensitivity of the type of FOUO information contained in the records.

(ii) Record copies of FOUO documents shall be disposed of in accordance with the disposal standards established under 44 U.S.C. chapter 33, as implemented by DCAAM 5015.1<sup>5</sup>, "Files Maintenance and Disposition Manual".

(3) Unauthorized Disclosure. The unauthorized disclosure of FOUO records does not constitute an unauthorized disclosure of DoD information classified for security purposes. Appropriate administrative action shall be

<sup>3</sup>See footnote 1 to paragraph (b)(3).

<sup>4</sup>See footnote 1 to paragraph (b)(3).

<sup>5</sup>See footnote 2 to paragraph (c)(2).

**Pt. 290, App. D**

**32 CFR Ch. I (7-1-10 Edition)**

taken, however, to fix responsibility for unauthorized disclosure whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The DCAA organizational element or DoD component that originated the FOUO information shall be informed of its unauthorized disclosure.

(g) Protection of Field Detachment Sensitive Information. (1) Definition. All communication, which qualifies for withholding under Exemptions (2) through (9), between regular DCAA organizational elements and Field Detachment offices is sensitive information and, as a minimum, shall be marked: FOR OFFICIAL USE ONLY (FOUO).

(2) Markings. (i) Communications, which qualify for withholding under Exemptions (2) through (9) initiated by a Field Detachment office, will bear the following marking:

**FOR OFFICIAL USE ONLY**

Access limited to addressee and his/her designated representative(s) with a need-to-know.

This document may not be reproduced or further disseminated without the approval of the Director, Field Detachment, DCAA.

(ii) All correspondence specifically exempt under Exemptions (2) through (9), including assist audit requests, generated by a regular (non-FD) DCAA office, which is addressed to the Field Detachment, either Headquarters or a field audit office, will be marked FOR OFFICIAL USE ONLY and will be limited within the FAO to one protected office copy.

(3) Storage. (i) All Field Detachment sensitive information in the possession of a regular DCAA office will be stored in a classified container, if available. If a classified container is not available, the sensitive information shall be stored in a locked container controlled by the FAO manager.

(ii) Permanent files currently maintained by regular DCAA offices, which are available to all FAO personnel, should not contain any detailed information on Field Detachment audit interest. That information shall be protected as sensitive information and stored in accordance with paragraph (g)(3)(i) of this appendix.

(4) Dissemination. (i) Access to Field Detachment sensitive information by other DCAA audit and administrative personnel within the office shall be on a strict need-to-know basis as determined by the FAO manager.

(ii) Requests by non-DCAA personnel for access to Field Detachment sensitive information must be coordinated with the Direc-

tor, Field Detachment, through Headquarters, DCAA.

[56 FR 49685, Oct. 1, 1991, as amended at 60 FR 18006, Apr. 10, 1995; 60 FR 35699, July 11, 1995]

**APPENDIX D TO PART 290—AUDIT  
WORKING PAPERS**

*(a) Definition*

(1) Audit working papers contain information from accounting and statistical records, personal observations, the results of interviews and inquiries, and other available sources. Audit working papers may also include contract briefs, copies of correspondence, excerpts from corporate minutes, organization charts, copies of written policies and procedures, and other substantiating documentation. The extent and arrangement of working paper files will depend to a large measure on the nature of the audit assignment.

(2) Working papers are generally classified in two categories: the permanent file and the current file.

*(i) Permanent file.*

(A) The permanent file on each contractor is a central repository of information gathered during the course of an audit which has continuing value and use to subsequent audits expected to be performed at the same contractor. Permanent files are useful in preparing the audit program and in determining the appropriate scope of subsequent audits. They also provide ready means for auditors to become familiar with the contractor's operations and any existing audit problems or contractor system weaknesses. While summary information on the contractor's organization, financial structure and policies may sometimes be included in permanent files for smaller contractors, such information on large contractors with continuing audit activity is generally maintained in the field audit office at the central reference library.

(B) Items which would logically be included in the permanent file as having continuing value in future audit assignments include:

(1) Internal control questionnaire.

(2) Internal control review update control log.

(3) Vulnerability assessment.

(4) MAARs control log.

(5) Disclosure statement and revisions in accordance with CAS rules and regulations, and

(6) CAS compliance control schedules and a noncompliance summary schedule.

(ii) Current File. The current file usually consists of working papers which have limited use on future assignments. DCAA Forms